

A Class of Profinite Hopf-Galois Extensions over \mathbb{Q}

Timothy Kohl

Department of Mathematics and Statistics

Boston University

Boston, MA 02215

tkohl@math.bu.edu

November 21, 2016

Abstract

For p a prime and $a \in \mathbb{Q}$, where a is not a p^n -th power of any rational number, the extension $\mathbb{Q}(w_n)/\mathbb{Q}$ where $w_n = \sqrt[p^n]{a}$ is separable but non-normal. The Hopf-Galois theory for separable extensions was determined by Greither and Pareigis, and the specific classification for radical extensions such as these by the author. In this work we extend this theory to a certain class of profinite extensions, namely those formed from the union of these $\mathbb{Q}(w_n)$. We construct a 'profinite' Hopf algebra which acts, and show that it satisfies a generalization of a result due to Hagenmüller and Pareigis on the structure of Hopf algebra forms of group algebras.

Key words: Hopf-Galois extension, Greither-Pareigis theory

MSC: 16W30, 12F10

Introduction

A separable field extension K/k is Hopf-Galois if there is k -Hopf algebra H as well as a k -algebra map $\mu : H \rightarrow \text{End}_k(K)$ such that for $h \in H$ and

$a, b \in K$, one has

$$\mu(h)(ab) = \sum_{(h)} \mu(h_{(1)})(a) \mu(h_{(2)})(b) \quad (1)$$

where for $\Delta : H \leftarrow H \otimes H$ the co-multiplication of H ,

$$\Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$$

and where μ induces a k -algebra isomorphism

$$1 \# \mu : K \# H \rightarrow \text{End}_k(K) \quad (2)$$

and

$$K^H = \{x \in K \mid \mu(h)(x) = \epsilon(h)x \ \forall h \in H\} = k \quad (3)$$

where $\epsilon : H \rightarrow k$ is the co-unit map of H . All these properties generalize what happens when K/k is Galois with $G = \text{Gal}(K/k)$ for then one may set $H = k[G]$ with $\Delta(g) = g \otimes g$ and $\epsilon(g) = 1$ and where the map $\mu : H \rightarrow \text{End}_k(K)$ is obvious. In this situation (1) is simply the multiplicative action of the group elements extended linearly to sums in H , (3) is due to $K^G = k$ and (2) is linear independence of characters. As such, a Hopf-Galois structure for some other Hopf algebra (where indeed K/k may not even be Galois in the first place) is a way to generalize these three fundamental aspects of ordinary (classical) Galois theory of fields. Indeed the case where K/k is separable, but *not* Galois is the starting point of the work of Greither and Pareigis [5]. The primordial example they begin with (and one which is, broadly generalized, part of the family of extensions we consider in this work) is $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ which is non-normal due to the lack of roots of unity in the ground field \mathbb{Q} of course. Nonetheless, a certain rank 3 Hopf algebra can be shown to act on this extension to make it Hopf-Galois. Rather than give the example as it is presented in [5] we shall look at all such radical extensions in general.

1 Greither-Pareigis Theory

The setup in [5] is as follows. For K/k a finite separable extension of fields, with Galois closure \tilde{K}/K , let $\Gamma = \text{Gal}(\tilde{K}/k)$ and $\Delta = \text{Gal}(\tilde{K}/K)$.

The natural action of Γ on the left cosets $S = \Gamma/\Delta$ yields a map $\lambda : \Gamma \rightarrow \text{Perm}(S) = B$. Note that for Δ trivial λ is the left regular representation of Γ in its group of permutations. Also one needs the following definition.

Definition 1.1: A regular subgroup $N \leq \text{Perm}(S)$ is one that acts transitively and fixed point freely on the elements of S . That is the orbit of any element of S under the action of N is all of S and if $n(s) = s$ for any $s \in S$ then n is the identity element.

A consequence of regularity is that for any such N , $|N| = |S|$. With these definitions in mind, one has

Theorem 1.2:[5, Theorem 2.1] *Given K/k and $B = \text{Perm}(\Gamma/\Delta)$ for Γ, Δ as above, the following are equivalent:*

(a) *There is a k -Hopf algebra H making K/k H -Galois.*

(b) *There is a regular subgroup $N \leq B$ such that $\lambda(\Gamma) \leq \text{Norm}_B(N)$*

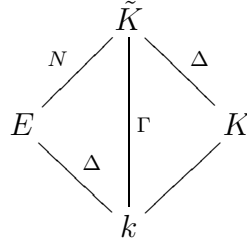
Moreover by Galois descent H can be shown to be $(\tilde{K}[N])^\Gamma$, the fixed ring under the diagonal (simultaneous) action of Γ on \tilde{K} (via the Galois action) and on N by conjugation in B by the elements of $\lambda(\Gamma)$.

The Hopf algebra given as the fixed ring has the further property that $\tilde{K} \otimes H \cong \tilde{K} \otimes k[N]$, that is, in the language of descent, H is a \tilde{K} -form of the group ring $k[N]$, i.e. the two k -Hopf algebras become isomorphic as \tilde{K} Hopf algebras. The enumeration of Hopf-Galois structures on a given K/k amounts to the enumeration of the regular subgroups of B normalized by $\lambda(\Gamma)$. Much recent work has focused on the case where K/k is already Galois with group Γ and therefore one is searching for regular subgroups of $\text{Perm}(\Gamma)$ normalized by the left-regular representation of Γ . However, we shall be considering cases closer in spirit to the original motivation for this subject, namely the construction of Hopf-Galois structures on non-normal separable extensions. Of particular relevance to the current discussion is the following class of extensions as defined in [5, Proposition 4.1]

Definition 1.3: If K/k is a separable extension with Γ and Δ as above then if there exists $N \triangleleft \Gamma$ such that $N \cap \Delta = \{e\}$ and $\Gamma = N\Delta$ (i.e. N is a normal complement to Δ in Γ) then K/k is Hopf-Galois for $H = (E[N^{\text{opp}}])^\Delta$ where

$E = \tilde{K}^N$ and $N^{opp} = \text{Cent}_B(N)$. Such a Hopf-Galois structure is termed *almost classical*.

This bears some exploration in terms of the construction of the Hopf algebra which acts. If N is a normal subgroup of Γ with fixed field E then have



where $\text{Gal}(E/k) \cong \Delta$ by natural irrationality. Observe that N being a normal subgroup of Γ means that, if we identify N with $\lambda(N)$ embedded in B that $\lambda(N)$ is normalized by $\lambda(\Gamma)$. Moreover, since N is a normal complement to Δ in Γ then (viewed inside B), N is regular. As such, N itself gives rise to a Hopf-Galois structure with Hopf algebra $(\tilde{K}[N])^\Gamma$. However, for N a regular subgroup it's readily shown that $N^{opp} = \text{Cent}_B(N)$ is also regular and moreover that $\text{Norm}_B(N) = \text{Norm}_B(N^{opp})$ which is a direct analogue of the relationship between the left and right regular representations of a group G in its group of permutation (whose common normalizer is the holomorph $\text{Hol}(G)$). The Hopf algebra that arises using N^{opp} is of course $(\tilde{K}[N^{opp}])^\Gamma$, but since $\Gamma = N\Delta$ and since N centralizes N^{opp} and has fixed field E then

$$(\tilde{K}[N^{opp}])^{N\Delta} = ((\tilde{K}[N^{opp}])^N)^\Delta = (E[N^{opp}])^\Delta$$

which is basically the observation made in [5, Corollary 3.2]. For the case where N is abelian then $N^{opp} = N$ and $H = (E[N])^\Delta$ whose action even more so merits the adjective *almost classical* since the action is based on the existence and action of a subgroup of the Galois closure of K/k . For the cases we shall be studying this will be the situation since N will be cyclic of prime power order. Indeed it is a natural extension of the author's work in [8] enumerating the Hopf-Galois structures on radical extensions $k(w)/k$ with $w \notin k$ where $\text{char}(k) = 0$ and $w^{p^n} = a \in k$ (p an odd prime) where k contains at most a p^r -th root of unity but not a p^{r+1} root of unity.

Theorem 1.4:[8, Theorem 3.3 and Theorem 4.5] *The radical extension $k(w)/k$*

given above has exactly p^r Hopf-Galois structures for $0 \leq r < n$ and p^{n-1} for $r = n$, of which $p^{\min(r, n-r)}$ are almost classical and for all, the associated group N is cyclic of order p^n .

Note that for $r = 0$ such a radical extension has exactly one Hopf-Galois structure, and it is almost classical.

2 Radical Extensions of \mathbb{Q}

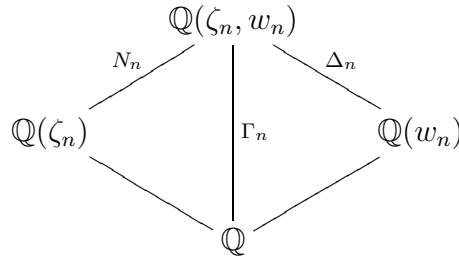
Here we shall consider the radical extensions $\mathbb{Q}(a^{1/p^n})/\mathbb{Q}$ for p an odd prime, where a is not a p^n -th power of any rational number. Since \mathbb{Q} contains no p^n -th roots of unity, these extensions are acted on by a unique Hopf algebra. We shall discuss their structure and how they relate to Greither-Pareigis theory and the study of Hopf algebra forms in [6]. Later, we shall construct a profinite Hopf algebra form that generalizes Theorem 5 of [6] and show that this form acts on the direct limit (union) of the extensions $\mathbb{Q}(a^{1/p^n})$. We will also view this action in terms of regularity to try and extend the results of Greither and Pareigis to such profinite separable extensions.

We shall use the following notation:

$$\begin{aligned} w_n &= a^{1/p^n}, a \in \mathbb{Q} \text{ (} a \text{ not already a } p^{n-\text{th}} \text{ power)} \\ \zeta_n &= \text{a primitive } p^{n-\text{th}} \text{ root of unity} \end{aligned}$$

$$\begin{aligned} N_n &= \text{Gal}(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_n)) \\ \Delta_n &= \text{Gal}(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(w_n)) \\ \Gamma_n &= \text{Gal}(\mathbb{Q}(w_n, \zeta_n)/\mathbb{Q}) \end{aligned}$$

which is diagrammed below.



Now $\mathbb{Q}(w_n)/\mathbb{Q}$ is a separable, non-normal extension which is H -Galois, for H exhibited below. Observe that $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is such that $\mathbb{Q}(\zeta_n)\mathbb{Q}(w_n) = \mathbb{Q}(\zeta_n, w_n)$ the normal closure of $\mathbb{Q}(w_n)/\mathbb{Q}$. Hence $\mathbb{Q}(w_n)/\mathbb{Q}$ is almost classically Galois. To compute the relevant Hopf algebra form we proceed as follows. There is a natural action:

$$\mathbb{Q}(\zeta_n)[N_n] \otimes \mathbb{Q}(\zeta_n, w_n) \longrightarrow \mathbb{Q}(\zeta_n, w_n)$$

Here $N_n = \langle \sigma_n \rangle$ is cyclic of order p^n where $\sigma_n(w_n) = \zeta_n w_n$ and $\Delta_n \cong \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. This, in turn, is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^\times$ via the homomorphism $t : \Delta_n \longrightarrow (\mathbb{Z}/p^n\mathbb{Z})^\times$ where, since $\Delta_n = \langle \delta_n \rangle$ is cyclic of order $\phi(p^n)$, we define $t(\delta_n) = \pi \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ a primitive root mod p^n . Furthermore $\Delta_n \cong \text{Aut}(N_n)$ via the map τ_n where we define $\tau_n(\delta_n)(\sigma_n^i) = \sigma_n^{it(\delta_n)} = \sigma_n^{i\pi}$. Moreover, since $\mathbb{Q}(w_n)$ and $\mathbb{Q}(\zeta_n)$ are linearly disjoint over \mathbb{Q} we have $\Gamma_n = N_n \Delta_n \cong N_n \rtimes \Delta_n$ and by natural irrationality Δ_n may be viewed as $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. We can define then an action (the diagonal action) of Δ_n on the group ring $\mathbb{Q}(\zeta_n)[N_n]$ as follows:

$$\delta_n(r\zeta_n^a\sigma_n^b) = r\zeta_n^{a\pi}\sigma_n^{b\pi} \text{ where } r \in \mathbb{Q}$$

Of course, Δ_n acts on $\mathbb{Q}(\zeta_n, w_n)$, so we may pass from:

$$\mathbb{Q}(\zeta_n)[N_n] \otimes \mathbb{Q}(\zeta_n, w_n) \longrightarrow \mathbb{Q}(\zeta_n, w_n)$$

by descent to the corresponding action:

$$(\mathbb{Q}(\zeta_n)[N_n])^{\Delta_n} \otimes (\mathbb{Q}(\zeta_n, w_n))^{\Delta_n} \longrightarrow (\mathbb{Q}(\zeta_n, w_n))^{\Delta_n}$$

By Theorem 5 of [6] we have that $(\mathbb{Q}(\zeta_n)[N_n])^{\Delta_n}$ is a $\mathbb{Q}(\zeta_n)$ -Hopf algebra form of $\mathbb{Q}N_n$, since $\Delta_n = \text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and $\text{Aut}(N_n) \cong \Delta_n$. We shall denote this Hopf algebra by H_n and since $\mathbb{Q}(\zeta_n) \otimes_{\mathbb{Q}} H_n \cong \mathbb{Q}(\zeta_n)[N_n]$, then $\text{rk}_{\mathbb{Q}}(H_n) = p^n$. That we have an action

$$H_n \otimes \mathbb{Q}(w_n) \longrightarrow \mathbb{Q}(w_n)$$

follows from [5, Proposition 4.1] which says that the almost classical extension $\mathbb{Q}(w_n)/\mathbb{Q}$ is Hopf-Galois for an E -Hopf algebra form of a $\mathbb{Q}N$ where $N = \text{Gal}(E/\mathbb{Q})$ is a normal complement to Δ_n inside Γ_n . However, again by [8, Theorem 3.7 and Theorem 4.5], the only such subgroup is N_n and so this is the only almost-classical structure for this extension.

2.1 H_n and how it acts

The Hopf algebra H_n is a fixed ring under the action of Δ_n as given above. We shall show that this is a relatively familiar object by constructing a basis for it.

Proposition 2.1: H_n is isomorphic to $(\mathbb{Q}N_n)^*$ the linear dual of the group ring.

Proof. We start by defining the elements:

$$e_{n,i} = \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} \sigma_n^j$$

for i from 0 to $p^n - 1$. For $\Delta_n = \langle \delta_n \rangle$ we have

$$\begin{aligned} \delta_n e_{n,i} &= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-\pi i j} \sigma_n^{\pi j} \\ &= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-i(\pi j)} \sigma_n^{(\pi j)} \\ &= e_{n,i} \end{aligned}$$

since $(\pi, p) = 1$. Therefore each $e_{n,i}$ is contained in H_n and to show that these comprise a basis for H_n we shall, along the way, identify H_n as a familiar object. Specifically, given $N_n = \langle \sigma \rangle$ we have the character group $\hat{N}_n = \langle \chi_n \rangle$ where $\chi_n^j(\sigma_n^k) = \zeta_n^{jk}$. In [2, Theorem 7.10] it is shown that for a connected commutative ring R , and finite abelian group G where $|G|$ is invertible in R that if R contains a primitive $\exp(G)^{th}$ root of unity that $R[G] \cong R[\hat{G}] \cong (R[G])^* = \text{Hom}_R(R[G], R)$. Our basis for H_n uses basically this result. Since N_n is cyclic, the map $\sigma_n \mapsto \chi_n$ is a group isomorphism which can be extended by linearity to an isomorphism (of rings) $\mathbb{Q}(\zeta)[N_n] \rightarrow \mathbb{Q}(\zeta)\hat{N}_n$. If we let Δ_n act on $\mathbb{Q}(\zeta)$ in the usual way and act on \hat{N}_n by $\delta_n \chi_n = \chi_n^\pi$ then the above isomorphism is Δ_n -equivariant. Under this

map, $e_{n,i} \mapsto \widehat{e}_{n,i}$ where $\widehat{e}_{n,i} = \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} \chi_n^j$ and we have then that

$$\begin{aligned} \widehat{e}_{n,i}(\sigma_n^k) &= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} \chi_n^j(\sigma_n^k) \\ &= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} \zeta_n^{kj} \\ &= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{j(k-i)} \\ &= \delta_{ik} \end{aligned}$$

That is, we may identify the $\widehat{e}_{n,i}$'s with the $e_{n,i}$ constructed earlier and in doing so identify the \mathbb{Q} span of these with $(\mathbb{Q}N_n)^*$, the \mathbb{Q} dual of the group ring $\mathbb{Q}N_n$. Since the isomorphism $\mathbb{Q}(\zeta)[N_n] \rightarrow \mathbb{Q}(\zeta)\widehat{N}_n$ is Δ_n -equivariant we conclude that $H_n \cong (\mathbb{Q}N_n)^*$.

□

This isomorphism is not unexpected in light of [5, p.247 Remark 2] where the authors observe (due to [3, p.39]) that if $X^n - a^n$ is irreducible over k then $k(a)/k$ is Hopf-Galois where the Hopf algebra acting is the dual of the group ring. From 1.4 we know that this is, of course, the *only* Hopf-Galois structure. The isomorphism of H_n with the dual of the group ring is not just merely a way to identify it with something familiar. It actually yields an interesting parallel when we look at how it acts on $\mathbb{Q}(w_n)$.

Proposition 2.2: *The action of H_n on $\mathbb{Q}(w_n)$ is as follows. If $i = 0, \dots, p^n - 1$ and $k = 0, \dots, p^n - 1$ then $e_{n,i}(w_n^k) = \delta_{ik} w_n^k$.*

Proof. A basis for $\mathbb{Q}(w_n)$ over \mathbb{Q} consists of powers w_n^k for k from 0 to $p^n - 1$.

Using the $e_{n,i}$ given earlier, where $i = 0, \dots, p^n - 1$, direct calculation yields

$$\begin{aligned}
e_{n,i}(w_n^k) &= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} \sigma_n^j(w_n^k) \\
&= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} (\zeta_n^{kj} w_n^k) \\
&= w_n^k \left[\frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij+kj} \right] \\
&= w_n^k \left[\frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{j(k-i)} \right] \\
&= \delta_{ik} w_n^k
\end{aligned}$$

□

As such, the $e_{n,i}$ are almost a 'dual basis' to $\{1, w_n, \dots, w_n^{p^n-1}\}$.

Now we know that H_n will be a form of $\mathbb{Q}[N_n]$ in that $\mathbb{Q}(\zeta_n) \otimes H_n \cong \mathbb{Q}(\zeta_n)[N_n]$ but it will also be important in the sequel to have some insight into the structure of $\mathbb{Q}(\zeta_m) \otimes H_n$ for different m . We have the following:

Lemma 2.3: *Given H_n as defined above, if $m \geq n$ then $\mathbb{Q}(\zeta_m) \otimes H_n \cong \mathbb{Q}(\zeta_m)[N_n]$ and if $m < n$ then $\mathbb{Q}(\zeta_m) \otimes H_n$ contains $\sigma_n^{p^{n-m}}$.*

Proof. For $m \geq n$ we have that $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_m)$ so that $\mathbb{Q}(\zeta_m) \otimes H_n = \mathbb{Q}(\zeta_m) \otimes (\mathbb{Q}(\zeta_n) \otimes H_n) = \mathbb{Q}(\zeta_m) \otimes (\mathbb{Q}(\zeta_n)[N_n]) = \mathbb{Q}(\zeta_m)[N_n]$.

If $m < n$ then $\mathbb{Q}(\zeta_m) \otimes H_n$ will not be the full group-ring since $\mathbb{Q}(\zeta_m)$ doesn't contain p^{n-th} roots of unity, so in particular it will not contain σ_n . However, using the basis $\{e_{n,i}\}$ for H_n together with the fact that $\zeta_m = (\zeta_n)^{p^{n-m}}$ we can show that this partial base extension of H_n contains $\sigma_n^{p^{n-m}}$.

Consider the following $\mathbb{Q}(\zeta_m)$ -linear combination of the $e_{n,i}$

$$\begin{aligned} \sum_{i=0}^{p^n-1} \zeta_n^{a_i p^{n-m}} e_{n,i} &= \sum_{i=0}^{p^n-1} \zeta_n^{a_i p^{n-m}} \left[\frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} \sigma_n^j \right] \\ &= \sum_{j=0}^{p^n-1} \left[\frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_n^{a_i p^{n-m}} \zeta_n^{-ij} \right] \sigma_n^j \\ &= \sum_{j=0}^{p^n-1} \left[\frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_n^{a_i p^{n-m} - ij} \right] \sigma_n^j \end{aligned}$$

where now the coefficient of $\sigma_n^{p^{n-m}}$ is

$$\frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_n^{(a_i - i)p^{n-m}}$$

which, if we choose $a_i = i$ for each i yields 1. And for $j \neq p^{n-m}$ one has

$$\frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_n^{i(p^{n-m}-j)}$$

where we may view the i as coming from \mathbb{Z}_{p^n} . As such if $p^{n-m} - j = p^k u$ where $\gcd(u, p) = 1$ then multiplication by $p^k u$ represents an onto homomorphism from $\mathbb{Z}_{p^n} \rightarrow \mathbb{Z}_{p^{n-k}}$ and since

$$\sum_{t \in \mathbb{Z}_{p^{n-k}}} \zeta_n^t = 0$$

then

$$\frac{1}{p^n} \sum_{i=0}^{p^n-1} \zeta_n^{i(p^{n-m}-j)} = 0$$

for $j \neq p^{n-m}$. Thus, this $\mathbb{Q}(\zeta_m)$ -linear combination of the $e_{n,i}$ is exactly $\sigma_n^{p^{n-m}}$. That $\mathbb{Q}(\zeta_m) \otimes H_n$ contains the unique order p^m subgroup of N_n is not a coincidence since one could, from the elements of $\langle \sigma_n^{p^{n-m}} \rangle$ and $\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_n)$ form a collection $\{e'_{m,i}\}$ whose \mathbb{Q} -span would be an $H'_m \subseteq H_n$ isomorphic to H_m where therefore $\mathbb{Q}(\zeta_m) \otimes H'_m \cong \mathbb{Q}(\zeta_m)[N_m]$. The point is, that this is the smallest subgroup of N_n which lies in $\mathbb{Q}(\zeta_m) \otimes H_n$. \square

It's also interesting to compare the extensions $\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(w_n)/\mathbb{Q}$. The extension $\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_n)$ is Galois with respect to the group N_n and therefore canonically Hopf-Galois with respect to the Hopf algebra $\mathbb{Q}(\zeta_n)[N_n]$. And we've now demonstrated that the extension $\mathbb{Q}(w_n)/\mathbb{Q}$ is Hopf-Galois with respect to H_n which is isomorphic to $(\mathbb{Q}N_n)^*$. The analogy being made here is to the natural irrationality $Gal(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(w_n)) \cong Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

It is also worth considering the induced isomorphism (in this case) of

$$\mathbb{Q}(w_n) \# H_n \cong End_{\mathbb{Q}}(\mathbb{Q}(w_n))$$

which is a consequence of $\mathbb{Q}(w_n)/\mathbb{Q}$ being Hopf-Galois with respect to H_n . The underlying algebra of $\mathbb{Q}(w_n) \# H_n$ is $\mathbb{Q}(w_n) \otimes H_n$ but where the multiplication is 'twisted' by the action of H_n on $\mathbb{Q}(w_n)$. Specifically

$$(a \# h)(b \# h') = \sum_{(h)} ah_{(1)}(b) \# h_{(2)}h'$$

$$\text{where } \Delta(h) = \sum_{(h)} h_{(1)} \otimes h_{(2)}$$

and for H_n one has

$$\Delta(e_{n,i}) = \sum_{\{s,t \mid s+t=i\}} e_{n,s} \otimes e_{n,t}$$

since H_n is dual to the group ring and the $e_{n,i}$ are the basis of this dual. Bear in mind also that

$$\begin{aligned} \dim_{\mathbb{Q}}(End_{\mathbb{Q}}(\mathbb{Q}(w_n))) &= \dim_{\mathbb{Q}}(\mathbb{Q}(w_n) \otimes H_n) \\ &= [\mathbb{Q}(w_n) : \mathbb{Q}] \cdot \dim_{\mathbb{Q}}(H_n) \\ &= p^{2n} \end{aligned}$$

where H_n is embedded as the span of the $\{e_{n,i}\}$ given above in 2.2 and $\mathbb{Q}(w_n)$ is embedded as those linear transformations induced by left multiplication by the basis elements $\{1, w_n, \dots, w_n^{p^n-1}\}$. As such $\{w_n^j \# e_{n,i}\}$ is a basis for $\mathbb{Q}(w_n) \# H_n$, where we may also view $End_{\mathbb{Q}}(\mathbb{Q}(w_n))$ as being spanned by these elements. Specifically we have

$$(w_n^j \# e_{n,i})(w_n^k) = \begin{cases} 0 & \text{if } i \neq k \\ w_n^{j+k} & \text{if } i = k \end{cases} \quad (4)$$

which yields the multiplication explicitly, in accordance with the formula above:

$$\begin{aligned}
(w_n^j \# e_{n,i})(w_n^k \# e_{n,l}) &= \sum_{\{s,t \mid s+t=l\}} w_n^j e_{n,s}(w_n^k) \# e_{n,t} e_{n,l} \\
&= \sum_{\{s,t \mid s+t=l\}} w_n^j (\delta_{s,k} w_n^k) \# \delta_{t,l} e_{n,t} \\
&= \begin{cases} w_n^{j+k} \# e_{n,l} & \text{if } k+l=i \\ 0 & \text{otherwise} \end{cases}
\end{aligned}$$

As an interesting computational sideline, there is a nice way to associate the actions of $e_{n,i}$ and w_n^j within $End_{\mathbb{Q}}(\mathbb{Q}(w_n))$ as matrices and the $w_n^j \# e_{n,i}$ as products of these matrices. We demonstrate this explicitly in the case $p=3$ and $n=1$.

Viewing $\{1, w, w^2\}$ as the basis for $\mathbb{Q}(w)$, each e_i can be represented as a 3×3 matrix which is zero except for the $i+1^{st}$ column which consists of the $i+1^{st}$ elementary basis vector for $V = \mathbb{Q}^3$. i.e. We're making the identification $End_{\mathbb{Q}}(\mathbb{Q}(w)) \cong End_{\mathbb{Q}}(V) \cong GL_3(\mathbb{Q})$. Similarly, we view w^i as left multiplication l_{w^i} for $i = 0, 1, 2$ which act to cyclically rotate the basis vectors $\{1, w, w^2\}$. This yields the following 6 matrices:

$$\begin{aligned}
l_1 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} & e_0 &= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \\
l_w &= \begin{bmatrix} 0 & 0 & a \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} & e_1 &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \\
l_{w^2} &= \begin{bmatrix} 0 & a & 0 \\ 0 & 0 & a \\ 1 & 0 & 0 \end{bmatrix} & e_2 &= \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}
\end{aligned}$$

which when multiplied in pairs $\{l_{w^j}e_i\}$ yield nine matrices

$$\left\{ \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \right. \\ \begin{bmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & a \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \\ \left. \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & a & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & a \\ 0 & 0 & 0 \end{bmatrix} \right\}$$

corresponding to the $\{w_n^j \# e_i\}$. Note also that this set is clearly a basis for the endomorphism ring since $\sum_{j,i} c_{j,i} l_{w^j} e_i$ equals

$$\begin{bmatrix} c_{0,0} & c_{2,1}a & c_{1,2}a \\ c_{1,0} & c_{0,1} & c_{2,2}a \\ c_{2,0} & c_{1,1} & c_{0,2} \end{bmatrix}$$

which, given that $a \in \mathbb{Q}$, gives every 3×3 matrix over \mathbb{Q} for unique choices of $\{c_{j,i}\}$. One sees the same motif for larger p and n , namely a $p^n \times p^n$ matrix where every entry above the main diagonal is multiplied by a .

3 Profinite Forms

In this section we shall construct a profinite Hopf algebra form that satisfies a generalization of the following:

Theorem 3.1:[6, Theorem 5] *Let G be a finitely generated group with finite automorphism group $F = \text{Aut}(G)$. Then there is a bijection between $\mathbf{Gal}(k, F)$ (extensions of k with Galois group F) and $\mathbf{Hopf}(k[G])$ (Hopf algebra forms of $k[G]$) which associates with each F -Galois extension K of k the Hopf algebra*

$$H = \left\{ \sum c_g g \in KG \mid \sum f(c_g) f(g) = \sum c_g g \text{ for all } f \in F \right\}$$

Furthermore, H is a K -form of $k[G]$ by the isomorphism

$$\omega : H \otimes K \cong KG, \quad \omega(h \otimes a) = ah$$

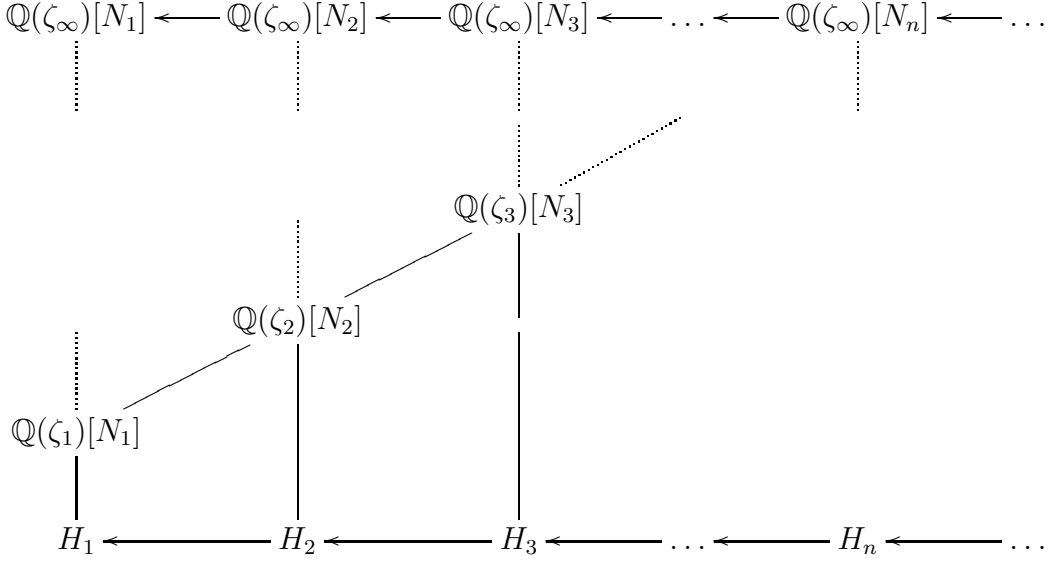
By construction, all the H_n are \mathbb{Q} -Hopf algebras which are $\mathbb{Q}(\zeta_n)$ -forms of the group rings $\mathbb{Q}[N_n]$ and are examples of the above theorem in action. The reason for this is that Δ_n is isomorphic to the automorphism group of the cyclic group N_n as well as to $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. What we would like to do now is to consider a profinite version of the above result. The usage of the term profinite is motivated by looking at the construction of the Galois group of a direct limit (union) of field extensions. In particular, for a base field F , if $L = \varinjlim K$ where K is a chain of sub-fields of L containing F , then if each K is a Galois extension of F then $\text{Gal}(L/F) = \varprojlim \text{Gal}(K/F)$ the inverse limit of the Galois groups of each of the K/F .

Here we shall consider the fields $\mathbb{Q}(w_n)$ where each w_n is chosen to be a p^n -th root of a fixed $a \in \mathbb{Q}$ which is not already a p^n -th root of a rational for any n . Even though these are not normal extensions of \mathbb{Q} , by what we have already shown each is Hopf-Galois over \mathbb{Q} with respect to the Hopf algebras H_n . As such, we will start with an inverse system using the H_n . The resulting Hopf algebra will be a form of a topologically finitely generated group whose automorphism group is not finite, but which satisfies the above theorem. That the automorphism group is infinite contrasts with the setup in [6].

One issue to be dealt with first is that, while the H_n are all \mathbb{Q} -Hopf algebras, the group rings $\mathbb{Q}(\zeta_n)[N_n]$ (which contain each H_n) are $\mathbb{Q}(\zeta_n)$ -Hopf algebras for each n . As such, one cannot start with a directed system involving these group rings, and then descend since these all lie in distinct categories of Hopf algebras, one for each ground field $\mathbb{Q}(\zeta_n)$.

As each H_n is $\mathbb{Q}(\zeta_n)$ -form of $\mathbb{Q}[N_n]$ then one may base change all H_n up to $\mathbb{Q}(\zeta_\infty)$ to yield group rings (and $\mathbb{Q}(\zeta_\infty)$ -Hopf algebras) $\mathbb{Q}(\zeta_\infty)[N_n]$, as

diagrammed below.



As such, we will define a pair of inverse systems of Hopf algebras over \mathbb{Q} and $\mathbb{Q}(\zeta_\infty)$ which will be related by descent.

Define $\nu_{j,i} : \mathbb{Q}(\zeta_\infty)[N_j] \longrightarrow \mathbb{Q}(\zeta_\infty)[N_i]$ for $j \geq i$ as follows:

$$\begin{aligned}\nu_{j,i}(q) &= q \text{ for } q \in \mathbb{Q}(\zeta_\infty) \\ \nu_{j,i}(\sigma_j) &= \sigma_i\end{aligned}$$

Hence $\nu_{i,i}$ is the identity map on $\mathbb{Q}(\zeta_\infty)[N_i]$ and $\nu_{j,i} \circ \nu_{k,j} = \nu_{k,i}$ for $k \geq j \geq i$ and we have the following obvious fact.

Lemma 3.2: $\nu_{j,i}$ is a surjective map of $\mathbb{Q}(\zeta_\infty)$ -Hopf algebras.

Proof. The surjectivity is obvious given that $\nu_{j,i}$ is surjective as a group homomorphism from N_j to N_i which, since it acts as the identity on the coefficients, is also seen to be a Hopf algebra morphism between the respective group rings. \square

We also need to consider whether the $\nu_{j,i}$ restrict to the H_n . As each $H_n \subseteq \mathbb{Q}(\zeta_n)[N_n] \subseteq \mathbb{Q}(\zeta_\infty)[N_n]$ is the span of $\{e_{n,i}\}$ given in 2.1 then it makes sense to compute $\nu_{n,n-1}(e_{n,i})$.

Lemma 3.3: For $e_{n,i}$ where $i \in \mathbb{Z}_{p^n}$ as given in 2.1, then

$$\nu_{n,n-1}(e_{n,i}) = \begin{cases} e_{n-1,i/p} & \text{if } i \in p\mathbb{Z}_{p^{n-1}} \subseteq \mathbb{Z}_{p^n} \\ 0 & \text{otherwise} \end{cases}$$

Proof. We have

$$e_{n,i} = \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} \sigma_n^j$$

so that, if $i \in p\mathbb{Z}_{p^{n-1}}$ then

$$\begin{aligned} \nu_{n,n-1}(e_{n,i}) &= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} \sigma_{n-1}^j \\ &= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_{n-1}^{-\frac{i}{p}j} \sigma_{n-1}^j \\ &= \frac{p}{p^n} \left(\sum_{j=0}^{p^{n-1}-1} \zeta_{n-1}^{-\frac{i}{p}j} \sigma_{n-1}^j \right) \\ &= e_{n-1,i/p} \end{aligned}$$

where the passage from ζ_n to ζ_{n-1} is due to the fact that i is a multiple of p . Since each $j \in \mathbb{Z}_{p^n}$ can be written as $ap^{n-1} + b$ where $a \in \mathbb{Z}_p$ and $b \in \mathbb{Z}_{p^{n-1}}$,

then if i is not a multiple of p we have

$$\begin{aligned}
\nu_{n,n-1}(e_{n,i}) &= \frac{1}{p^n} \sum_{j=0}^{p^n-1} \zeta_n^{-ij} \sigma_{n-1}^j \\
&= \frac{1}{p^n} \sum_{b=0}^{p^{n-1}-1} \sum_{a=0}^{p-1} \zeta_n^{-i(ap^{n-1}+b)} \sigma_{n-1}^{ap^{n-1}+b} \\
&= \frac{1}{p^n} \sum_{b=0}^{p^{n-1}-1} \sum_{a=0}^{p-1} \zeta_n^{-i(ap^{n-1}+b)} \sigma_{n-1}^b \\
&= \frac{1}{p^n} \sum_{b=0}^{p^{n-1}-1} \zeta_n^{-ib} \left(\sum_{a=0}^{p-1} \zeta_n^{-i(ap^{n-1})} \right) \sigma_{n-1}^b \\
&= \frac{1}{p^n} \sum_{b=0}^{p^{n-1}-1} \zeta_n^{-ib} \left(\sum_{a=0}^{p-1} \zeta_1^{-ia} \right) \sigma_{n-1}^b \\
&= \frac{1}{p^n} \sum_{b=0}^{p^{n-1}-1} \zeta_n^{-ib} (0) \sigma_{n-1}^b \\
&= 0.
\end{aligned}$$

□

It is interesting to note that, $\nu_{n,n-1} : H_n \rightarrow H_{n-1}$ where $H_n = (\mathbb{Q}N_n)^*$ and $H_{n-1} = (\mathbb{Q}N_{n-1})^*$ can be viewed as the dual of the natural map $\alpha_{n-1,n} : \mathbb{Q}N_{n-1} \rightarrow \mathbb{Q}N_n$ given by $\alpha_{n-1,n}(\sigma_{n-1}) = \sigma_n^p$ since then $\alpha_{n-1,n}^*$ would be defined by $\alpha_{n-1,n}^*(e_{n,i})(\sigma_{n-1}^j) = e_{n,i}(\sigma_n^{pj}) = \delta_{i,pj}$. As such $\alpha_{n-1,n}^*(e_{n,i}) = 0$ if i is not a multiple of p , and if i were a multiple of p then $\alpha_{n-1,n}^*(e_{n,i}) = e_{n-1,i/p}$ which is exactly what we get with $\nu_{n,n-1}$.

The H_n are constructed as $(\mathbb{Q}(\zeta_n)[N_n])^{\Delta_n}$ where Δ_n acts diagonally on the scalars and group elements by virtue of it being $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ and isomorphic to $Aut(N_n)$. In a related way we will consider the action of $Gal(\mathbb{Q}(\zeta_\infty)/\mathbb{Q})$ on each $\mathbb{Q}(\zeta_\infty)[N_n]$. Define $\phi_{j,i} : \Delta_j \rightarrow \Delta_i$ ($j \geq i$) by $\phi_{j,i}(\delta_j) = \delta_i$. It is easy to verify that $\{\Delta_i, \phi_{j,i}\}$ is also an inverse system and we shall define

$$\Delta_\infty = \varprojlim \Delta_i$$

which, amongst other things, is the Galois group of the profinite extension $\mathbb{Q}(\zeta_\infty)/\mathbb{Q}$. Furthermore, if we restrict $\nu_{j,i}$ to the N_j then it is clear that $\{N_j, \nu_{j,i}\}$ is an inverse system and we shall define $N_\infty = \varprojlim N_j$. Each N_j is cyclic of order p^j and Δ_∞ is also the inverse limit of the automorphism groups of each N_j . Since a given primitive root $\pi \bmod p$ is also a primitive root $\bmod p^n$ then we can choose the Galois group of $\mathbb{Q}(\zeta_j)$ to be generated by an element which acts to raise ζ_j to π for all j . Similarly, each automorphism group is generated by an element which acts to raise σ_n to the same power as well. We have the following which is known, for example [4, p.656], but we present here for use later.

Proposition 3.4:

$$\begin{aligned}
N_\infty &\cong \{ \{ \sigma_j^{a_j} \} \in \prod_{j=1}^\infty N_j \mid \nu_{j,i}(\sigma_j^{a_j}) = \sigma_i^{a_i} \pmod{p^i} \} \\
&\cong \{ \{ \sigma_j^{a_j} \} \in \prod_{j=1}^\infty N_j \mid a_j \equiv a_i \pmod{p^i} \} \\
&\cong J_p \text{ the } p\text{-adic integers} \\
\Delta_\infty &\cong \{ \{ \delta_i^{e_i} \} \in \prod_{j=1}^\infty \Delta_j \mid \phi_{j,i}(\delta_j^{e_j}) = \delta_i^{e_i} \} \\
&\cong \{ \{ \delta_i^{e_i} \} \in \prod_{j=1}^\infty \Delta_j \mid e_j \equiv e_i \pmod{p^i} \} \\
&\cong (J_p)^* \text{ the unit } p\text{-adic integers}
\end{aligned}$$

Note, exponents a_j in the definition of N_∞ lie in \mathbb{Z}_p whereas the e_j in the definition of Δ_∞ lie in $(\mathbb{Z}_p)^*$. And since component-wise Δ_j is the automorphism group of each N_j , then the congruence conditions on the respective exponents a_j and e_j yield the following which is also known.

Proposition 3.5: $\text{Aut}(N_\infty) \cong \Delta_\infty$

This could also be deduced from the fact that $\text{Aut}(\mathbb{Z}_p) \cong (\mathbb{Z}_p)^*$. Moreover, this implies that Δ_∞ acts by restriction on each N_i as $\text{Aut}(N_i)$. As such, Δ_∞ acts on each $\mathbb{Q}(\zeta_\infty)[N_i]$ which yields the following.

Lemma 3.6: *The following diagram commutes:*

$$\begin{array}{ccc} \mathbb{Q}(\zeta_\infty)[N_j] & \xrightarrow{\nu_{j,i}} & \mathbb{Q}(\zeta_\infty)[N_i] \\ \delta_j \downarrow & & \downarrow \delta_i \\ \mathbb{Q}(\zeta_\infty)[N_j] & \xrightarrow{\nu_{j,i}} & \mathbb{Q}(\zeta_\infty)[N_i] \end{array}$$

Lemmas 3.2, 3.3, and 3.6 imply that

$$\{\mathbb{Q}(\zeta_\infty)[N_j]\} \text{ and } \{(\mathbb{Q}(\zeta_\infty)[N_j])^{\Delta_\infty}\} \text{ and } \{H_j\}$$

are inverse systems with respect to $\nu_{j,i}$ where we have:

$$\varprojlim \mathbb{Q}(\zeta_\infty)[N_j] = \mathbb{Q}(\zeta_\infty)[N_\infty]$$

and if we define

$$H_\infty = \varprojlim H_j$$

we ask what the relationship is between $\mathbb{Q}(\zeta_\infty)[N_\infty]$ and H_∞ ?

We have the following:

Theorem 3.7:

- (a) $\mathbb{Q}(\zeta_\infty) \otimes_{\mathbb{Q}} H_\infty \cong \mathbb{Q}(\zeta_\infty)[N_\infty]$
- (b) $H_\infty = (\mathbb{Q}(\zeta_\infty)[N_\infty])^{\Delta_\infty}$

Proof. That Δ_∞ acts on $\mathbb{Q}(\zeta_\infty)[N_\infty]$ is clear given the previous observations that Δ_∞ is isomorphic to $Gal(\mathbb{Q}(\zeta_\infty)/\mathbb{Q})$ and $Aut(N_\infty)$. Moreover by 3.6 we have that $\delta_i(\nu_{j,i}(x)) = \nu_{j,i}(\delta_j(x)) = \nu_{j,i}(\phi_{j,i}(\delta_i)(x))$ for all $x \in \mathbb{Q}(\zeta_j)[N_j]$. (i.e. we may think of the $\nu_{j,i}$'s as Δ_∞ -maps) By virtue of 3.2 and 3.6 we have:

$$\begin{array}{ccccccc} H_1 & \xleftarrow{\nu_{2,1}} & H_2 & \xleftarrow{\nu_{3,2}} & \dots & \xleftarrow{\nu_{n,n-1}} & H_n & \xleftarrow{\nu_{n+1,n}} & \dots \\ & \searrow \psi_1 & \uparrow \psi_2 & & & \nearrow \psi_n & & & \\ & & H_\infty & & & & & & \end{array}$$

where the ψ_i are the canonical projections out of the direct limit. If we base change the above up to $\mathbb{Q}(\zeta_\infty)$ then we have the following:

$$\begin{array}{ccccccc} \mathbb{Q}(\zeta_\infty) \otimes H_1 & \xleftarrow{\nu_{2,1} \otimes 1} & \mathbb{Q}(\zeta_\infty) \otimes H_2 & \xleftarrow{\nu_{3,2} \otimes 1} & \dots & \xleftarrow{\psi_n \otimes 1} & \mathbb{Q}(\zeta_\infty) \otimes H_n \xleftarrow{\dots} \\ & \searrow \psi_1 \otimes 1 & \uparrow \psi_2 \otimes 1 & & & & \nearrow \\ & & \mathbb{Q}(\zeta_\infty) \otimes H_\infty & & & & \end{array}$$

But since $\mathbb{Q}(\zeta_n) \otimes_{\mathbb{Q}} H_n \cong \mathbb{Q}(\zeta_n)[N_n]$ and since $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_\infty)$ for all n then the above diagram becomes:

$$\begin{array}{ccccccc} \mathbb{Q}(\zeta_\infty)N_1 & \xleftarrow{\nu_{2,1} \otimes 1} & \mathbb{Q}(\zeta_\infty)N_2 & \xleftarrow{\nu_{3,2} \otimes 1} & \dots & \xleftarrow{\psi_n \otimes 1} & \mathbb{Q}(\zeta_\infty)N_n \xleftarrow{\dots} \\ & \searrow \psi_1 \otimes 1 & \uparrow \psi_2 \otimes 1 & & & & \nearrow \\ & & \mathbb{Q}(\zeta_\infty) \otimes H_\infty & & & & \end{array}$$

In general, direct limits 'commute' with the taking of tensor products, but the same is not true generally for inverse limits, since tensor product does not usually commute with direct products. However, we can 'build up' to $\mathbb{Q}(\zeta_\infty) \otimes H_\infty$ by first looking at $\mathbb{Q}(\zeta_m) \otimes \Pi_{n \geq 1} H_n$ where each $\mathbb{Q}(\zeta_m)$ is certainly finitely generated and projective as a \mathbb{Q} -module. As such, by [10, Prop. 1.1] the canonical map $\mathbb{Q}(\zeta_m) \otimes \Pi_{n \geq 1} H_n \rightarrow \Pi_{n \geq 1} \mathbb{Q}(\zeta_m) \otimes H_n$ is a bijection. By 2.3 we have that $\mathbb{Q} \otimes H_n$ contains $\mathbb{Q}(\zeta_m)[\langle \sigma_n^{p^{n-m}} \rangle]$. And since tensor product *does* commute with direct limits, we have

$$\begin{aligned} \mathbb{Q}(\zeta_\infty) \otimes \Pi_{n \geq 1} H_n &\cong (\varinjlim_m \mathbb{Q}(\zeta_m)) \otimes \Pi_{n \geq 1} H_n \\ &\cong \varinjlim_m (\mathbb{Q}(\zeta_m) \otimes \Pi_{n \geq 1} H_n) \\ &\cong \varinjlim_m (\Pi_{n \geq 1} \mathbb{Q}(\zeta_m) \otimes H_n) \end{aligned}$$

where now, viewing the direct limit as union, we have that each component in the direct product $\mathbb{Q}(\zeta_\infty) \otimes \Pi_{n \geq 1} H_n$ is exactly $\mathbb{Q}(\zeta_\infty)[N_n]$. So, within this direct product, we have the sub-algebra determined by the $\nu_{n,n-1}$ which is the inverse limit of $\mathbb{Q}(\zeta_\infty)[N_n]$, that is

$$\mathbb{Q}(\zeta_\infty) \otimes_{\mathbb{Q}} H_\infty = \mathbb{Q}(\zeta_\infty) \otimes_{\mathbb{Q}} (\varprojlim H_n) = \varprojlim (\mathbb{Q}(\zeta_\infty)[N_n]) = \mathbb{Q}(\zeta_\infty)[N_\infty]$$

which completes the proof of (a).

To show (b) we shall use the canonical constructions of $\varprojlim(\mathbb{Q}(\zeta_\infty)N_j) = \mathbb{Q}(\zeta_\infty)[N_\infty]$ and $\varprojlim H_i = H_\infty$. We have

$$\begin{aligned}\mathbb{Q}(\zeta_\infty)[N_\infty] &\cong \{ \{ \gamma_j \} \in \prod_{j=1}^\infty \mathbb{Q}(\zeta_\infty)[N_j] \mid \nu_{j,i}(\gamma_j) = \gamma_i \} \\ H_\infty &\cong \{ \{ \gamma_j \} \in \prod_{j=1}^\infty H_j \mid \nu_{j,i}(\gamma_j) = \gamma_i \}\end{aligned}$$

where the usage of γ_j in both is not an abuse of notation since $H_j \subseteq \mathbb{Q}(\zeta_\infty)[N_j]$ for each j and so also there is containment of the direct products.

Now if $\hat{\delta} = \{ \delta_j^{e_j} \} \in \Delta_\infty$ and $\{ \gamma_j \} \in \mathbb{Q}(\zeta_\infty)[N_\infty]$ then $\{ \gamma_j \}^{\hat{\delta}} = \{ \gamma_j \}$ implies that $\delta_j^{e_j}(\gamma_j) = \gamma_j$ for all j . The question is does this imply that $\gamma_j \in H_j$ for all $j \geq 1$? Yes, because Δ_∞ contains $\{ \delta_j^{e_j} \}$ where $e_j = 1$ for any specified $j \geq 1$, so indeed $\delta_j(\gamma_j) = \gamma_j$ for each $j \geq 1$ and therefore $\{ \gamma_j \} \in \prod_{j=1}^\infty H_j$. But now, since $\{ \gamma_j \} \in \mathbb{Q}(\zeta_\infty)[N_\infty]$ we have $\nu_{j,i}(\gamma_j) = \gamma_i$ so when restricted to $\gamma_j \in H_j$ we have $\{ \gamma_j \} \in H_\infty$. Thus $(\mathbb{Q}(\zeta_\infty)[N_\infty])^{\Delta_\infty} \subseteq H_\infty$.

The other inclusion is obvious since $H_\infty \subseteq \mathbb{Q}(\zeta_\infty)[N_\infty]$ and is fixed by all of $\prod_{j=1}^\infty \Delta_j$, so therefore by Δ_∞ . \square

One should note that H_∞ is generated by $\{ e_{n,i_n} \}$ (in the direct product) where $i_n = p \cdot i_{n-1}$ which makes sense if we go back to the observation earlier that each H_n is isomorphic to $(\mathbb{Q}N_n)^*$ where now

$$\begin{aligned}H_\infty &\cong \varprojlim (\mathbb{Q}[N_n])^* \\ &= \varprojlim \text{Hom}(\mathbb{Q}[N_n], \mathbb{Q}) \\ &\cong \text{Hom}(\varinjlim \mathbb{Q}[N_n], \mathbb{Q})\end{aligned}$$

where $\varinjlim \mathbb{Q}[N_n]$ is the group ring over the p -Prüfer group formed from the union of the $\{ N_n \}$ since each are cyclic of order p^n . It is also interesting to note that (again as cited in [4]) the automorphism group of the p -Prüfer group is also isomorphic to $\Delta_\infty \cong (J_p)^*$. Undoubtedly, this is obliquely a manifestation/result of the fact (cited in [1] for example) that J_p and the p -Prüfer group are Pontryagin duals of each other. That H_∞ is a Hopf algebra

is a consequence of the fact that $\mathbb{Q}(\zeta_\infty)/\mathbb{Q}$ (being a direct limit of faithfully flat extensions) is a faithfully flat extension so by general descent theory [9] such an extension preserves and reflects structures such as Hopf algebras. That is, since H_∞ is a $\mathbb{Q}(\zeta_\infty)$ form of $\mathbb{Q}[N_\infty]$ which is a Hopf algebra then H_∞ is a Hopf algebra over \mathbb{Q} . This is also a rare example of where the dual of an infinite dimensional Hopf algebra is itself a Hopf algebra since typically one loses the 'closure' of the induced co-algebra structure on the dual in this setting. Aside from this descent theoretic proof of this fact, it is the author's conjecture that H_∞ is Hopf, even though it is the dual of an infinite group, since said infinite group is torsion. That is the finite dual is the dual.

Additionally, in view of 3.5 and that $\text{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) = \Delta_\infty$, this yields a nice generalization of Theorem 5 of [6].

4 $\mathbb{Q}(w_\infty)/\mathbb{Q}$ as an H_∞ -Galois extension

The field $\mathbb{Q}(w_\infty)$ is certainly linearly disjoint to $\mathbb{Q}(\zeta_\infty)$ over \mathbb{Q} . Moreover, the normal closure of $\mathbb{Q}(w_\infty)$ contains $\mathbb{Q}(\zeta_\infty)\mathbb{Q}(w_\infty)$ since the splitting field for all polynomials of the form $x^{p^n} - a$ must contain $\mathbb{Q}(\zeta_\infty)$ and $\mathbb{Q}(w_\infty)$. It then must be contained in $\mathbb{Q}(\zeta_\infty)\mathbb{Q}(w_\infty)$ since the minimal polynomial of any element in $\mathbb{Q}(w_\infty)$ is split in $\mathbb{Q}(\zeta_\infty)\mathbb{Q}(w_\infty)$. The question is, can we view $\mathbb{Q}(w_\infty)/\mathbb{Q}$ as a Hopf-Galois extension with respect to the action of H_∞ ?

The difficulty that arises is in verifying that H_∞ acts on $\mathbb{Q}(w_\infty)$ in the same way that a profinite Galois group would act on a direct limit (union) of the intermediate fields. Since $\mathbb{Q}(w_\infty)$ is the direct limit (union) over all $\mathbb{Q}(w^{p^n}) \subseteq \mathbb{Q}(w_\infty)$ then if it were a normal extension, its Galois group would be the inverse limit of the Galois groups of each intermediate field over \mathbb{Q} . We have that for each n there is an isomorphism $\mathbb{Q}(w_n) \# H_n \cong \text{End}_{\mathbb{Q}}(\mathbb{Q}(w_n))$ and since $\mathbb{Q}(w_\infty) = \varinjlim \mathbb{Q}(w_n)$ then we wish to examine the relationships between $\text{End}_{\mathbb{Q}}(\mathbb{Q}(w_\infty))$ and $\mathbb{Q}(w_\infty) \# H_\infty$.

We first observe that

$$\begin{aligned}
\text{End}(\mathbb{Q}(w_\infty)) &= \text{Hom}(\varinjlim_n \mathbb{Q}(w_n), \varinjlim_m \mathbb{Q}(w_m)) \\
&\cong \varprojlim_n \text{Hom}(\mathbb{Q}(w_n), \varinjlim_m \mathbb{Q}(w_m)) \\
&\cong \varprojlim_n \left[\varinjlim_m \text{Hom}(\mathbb{Q}(w_n), \mathbb{Q}(w_m)) \right]
\end{aligned}$$

where the direct limit (over n) in the first component becomes the inverse limit induced by the natural restriction map

$$\text{Hom}(\mathbb{Q}(w_n), \varinjlim_m \mathbb{Q}(w_m)) \longrightarrow \text{Hom}(\mathbb{Q}(w_{n-1}), \varinjlim_m \mathbb{Q}(w_m))$$

since $\mathbb{Q}(w_{n-1}) \subseteq \mathbb{Q}(w_n)$. The direct limit (over m) from the second component is permitted to be moved outside due to the fact that $\mathbb{Q}(w_n)$ is finitely presented for each n .

Proposition 4.1: *The algebra $\text{Hom}(\mathbb{Q}(w_n), \mathbb{Q}(w_m))$ is isomorphic to*

(a) $\mathbb{Q}(w_m) \# \overline{H}_{m,n}$ where $\overline{H}_{m,n}$ is the sub-algebra of H_m spanned by $\{e_{m,i}\}$ for $i \in p^{m-n}\mathbb{Z}_{p^n} \subseteq \mathbb{Z}_{p^m}$ if $m \geq n$ or

(b) the sub-algebra of $\mathbb{Q}(w_n) \# H_n$ spanned by $\{w_n^j \# e_{n,i}\}$ where $i \in \mathbb{Z}_{p^n}$ where $p^{n-m} \mid j+i$ if $m < n$.

Proof. If $m \geq n$ then $\text{Hom}(\mathbb{Q}(w_n), \mathbb{Q}(w_m)) \subseteq \text{Hom}(\mathbb{Q}(w_m), \mathbb{Q}(w_m))$ where the latter is isomorphic to $\mathbb{Q}(w_m) \# H_m$. As given in (4),

$$(w_m^j \# e_{m,i})(w_m^{tp^{m-n}}) = \begin{cases} 0 & i \neq tp^{m-n} \\ w_m^{j+tp^{m-n}} & i = tp^{m-n} \end{cases}$$

so those elements of $\mathbb{Q}(w_m) \# H_m$ that have domain $\mathbb{Q}(w_n) = \mathbb{Q}((w_m)^{p^{m-n}})$ are exactly $w_m^j \# e_{m,i}$ for $i \in p^{m-n}\mathbb{Z}_{p^n} \subseteq \mathbb{Z}_{p^m}$. If one views these as $p^m \times p^m$ matrices, then this sub-algebra consists of those matrices where (if numbering columns from 0) have non-zero columns if the column index is in $p^{m-n}\mathbb{Z}_{p^n} \subseteq \mathbb{Z}_{p^m}$.

If $m < n$ then $w_m = w_n^{p^{n-m}}$ and so $Hom(\mathbb{Q}(w_n), \mathbb{Q}(w_m)) \subseteq Hom(\mathbb{Q}(w_n), \mathbb{Q}(w_n))$ where the latter is isomorphic to $\mathbb{Q}(w_n) \# H_n$. However, here the co-domain is restricted to $\mathbb{Q}(w_m) \subseteq \mathbb{Q}(w_n)$ so any w_n^t must map to $\mathbb{Q}(w_m)$. Again, by (4),

$$(w_n^j \# e_{n,i})(w_n^t) = \begin{cases} 0 & i \neq t \\ w_n^{j+t} & i = t \end{cases}$$

so as t varies over \mathbb{Z}_{p^n} so must i which means j is restricted by the condition that $j + t$ must be a multiple of p^{n-m} which means $p^n \cdot p^m$ choices for (j, i) which is dimensionally correct given the domain and co-domain of the homomorphisms in question. \square

If one now considers the direct limit

$$\lim_{\rightarrow m} Hom(\mathbb{Q}(w_n), \mathbb{Q}(w_m))$$

for a given n , then one is looking at endomorphisms of $\mathbb{Q}(w_m)$, generated by left multiplication by elements of $\mathbb{Q}(w_m)$ together with those arising from each sub-algebra, either H_n (when $m < n$) or $\overline{H}_{m,n}$ for those $m \geq n$. If for notational uniformity we define $\overline{H}_{m,n} = H_n$ when $m < n$ then we wish to first consider the direct limit $\lim_{\rightarrow m} \overline{H}_{m,n}$.

Although we are considering the action on $\mathbb{Q}(w_\infty)$ by H_∞ , which is the inverse limit of the H_m , there is a natural embedding of H_m into H_{m+1} via $e_{m,i} \mapsto e_{m+1,pi}$. Concordantly, for $m \geq n$ this restricts to an embedding $\overline{H}_{m,n} \hookrightarrow \overline{H}_{m+1,n}$ for each n since if $i \in p^{m-n}\mathbb{Z}_{p^n}$ then $pi \in p^{m+1-n}\mathbb{Z}_{p^n}$. However, this embedding is, in fact, an isomorphism since $\dim(\overline{H}_{m,n}) = p^n$ for each m ! Moreover, for each $m < n$, $\overline{H}_{m,n} = H_n$ so that, in fact:

$$\lim_{\rightarrow m} \overline{H}_{m,n} \cong H_n$$

and since the union of the scalars $\mathbb{Q}(w_m)$ is $\mathbb{Q}(w_\infty)$ then we have proved:

Proposition 4.2:

$$\lim_{\rightarrow m} Hom(\mathbb{Q}(w_n), \mathbb{Q}(w_m)) \cong \mathbb{Q}(w_\infty) \# H_n$$

This leads us to the main result for this section.

Theorem 4.3:

$$\text{End}(\mathbb{Q}(w_\infty), \mathbb{Q}(w_\infty)) \cong \mathbb{Q}(w_\infty) \# H_\infty$$

Proof. The principal observation needed is that the inverse limit

$$\begin{aligned} & \varprojlim_n \text{Hom}(\mathbb{Q}(w_n), \mathbb{Q}(w_\infty)) \\ & \cong \varprojlim_n \mathbb{Q}(w_\infty) \# H_n \end{aligned}$$

arises from the natural restriction maps, but these correspond exactly to the $\nu_{n,n-1}$ given earlier in the construction of H_∞ which act as the identity on $\mathbb{Q}(w_\infty)$, that is:

$$\varprojlim_n \mathbb{Q}(w_\infty) \# \overline{H}_n \cong \mathbb{Q}(w_\infty) \# H_\infty$$

so that the endomorphism ring of $\mathbb{Q}(w_\infty)$ is the latter smash product, making $\mathbb{Q}(w_\infty)/\mathbb{Q}$ a Hopf-Galois extension with respect to the action of H_∞ . \square

The last consideration is if H_∞ can be viewed within the Greither-Pareigis theory. We have that H_∞ is a $\mathbb{Q}(\zeta_\infty)$ -form (and therefore a $\mathbb{Q}(w_\infty, \zeta_\infty)$ -form) of the group ring $\mathbb{Q}N_\infty$. In terms of normal complements involving the Galois groups of the relevant intermediate extensions, namely

$$\begin{aligned} N_\infty &= \text{Gal}(\mathbb{Q}(w_\infty, \zeta_\infty)/\mathbb{Q}(\zeta_\infty)) \\ \Delta_\infty &= \text{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) \\ N_\infty \Delta_\infty &= \text{Gal}(\mathbb{Q}(w_\infty)\mathbb{Q}(\zeta_\infty)/\mathbb{Q}) \end{aligned}$$

the extension $\mathbb{Q}(w_\infty)/\mathbb{Q}$ is almost classical. (i.e. ' N ' is N_∞) The delicate part is if N_∞ can be viewed as a regular subgroup, and moreover, of what

ambient symmetric group? The construction of H_∞ parallels that of a profinite Galois group acting on a direct limit (union) of field extensions, where the restriction to a given sub-field in the chain corresponds to the action of the Galois group acting on that field extension. Here, H_∞ acts by restriction on $\mathbb{Q}(w_n)$ as H_n where, by Greither-Pareigis, there is a corresponding regular subgroup of $N_n \leq \text{Perm}(\Gamma_n/\Delta_n)$. Observe however that, as seen earlier, $\Gamma_n = N_n\Delta_n$ so that $\Gamma_n/\Delta_n = \{\sigma_n^i\Delta_n\}$ and where N_n acts naturally on the left, just as it would act on itself via the left regular representation. (i.e. identify $\text{Perm}(\Gamma_n/\Delta_n) \cong \text{Perm}(N_n)$) In the limit, the analogue would be N_∞ a regular subgroup of $\text{Perm}(N_\infty\Delta_\infty/\Delta_\infty) \cong \text{Perm}(N_\infty)$, via the left action, given that the left regular representation is the canonical example of a regular permutation group.

As such, in any related construction of an inverse limit of Hopf algebras acting on intermediate extensions, we should expect the restriction to any intermediate extension to also give rise to a regular subgroup embedded in the corresponding ambient symmetric group. And for the resulting Hopf algebra to be a form of a group ring over a profinite group, similarly embedded in the corresponding (infinite) ambient symmetric group.

5 Other Radical Extensions

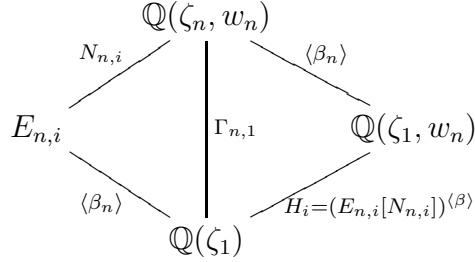
As given in 1.4, for a radical extension of the form $k(w)/k$, as one increases the number of p -th power roots of unity in the base field, the number of Hopf-Galois structures, including the number of almost classical structures increases as well. For example, $\mathbb{Q}(\zeta_1, w_n)/\mathbb{Q}(\zeta_1)$ has p Hopf-Galois structures, all $p^{\min(1, n-1)} = p^1 = p$ of which are almost classical. Moreover, the N 's which arise are all cyclic of order p^n . For the case of $\mathbb{Q}(\zeta_1, w_n)/\mathbb{Q}(\zeta_1)$ we have

$$\Gamma_{n,1} = \text{Gal}(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_1)) = \langle \sigma_n, \beta_n \rangle$$

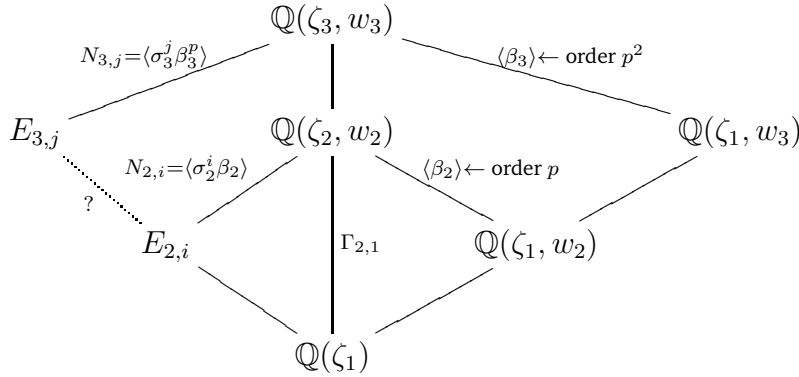
where $\langle \sigma_n \rangle = \text{Gal}(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_n))$ which we shall denote by $N_{n,0}$, which is cyclic of order p^n , of course, and $\langle \beta_n \rangle = \text{Gal}(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_1, w_n))$, which is cyclic of order p^{n-1} . We note, in passing, that $\Gamma_{n,1}$ is the Sylow p -subgroup of $\text{Gal}(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q})$ since $\langle \beta_n \rangle$ is the Sylow p -subgroup of $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$.

One can show (by [8, Theorem 3.3]) that $N_{n,0}$ and $N_{n,i} = \langle \sigma^i \beta^{p^{n-2}} \rangle$ for

$i \in U_p$ are the p different normal complements to $\langle \beta_n \rangle$ in $\Gamma_{n,1}$, all of which are cyclic of order p^n of course. If we denote by $E_{n,i} = (\mathbb{Q}(\zeta_n, w_n))^{N_i}$ then $\mathbb{Q}(\zeta_1, w_n)/\mathbb{Q}(\zeta_1)$ is Hopf-Galois with respect to the action of $H_{n,i} = (E_i[N_{n,i}])^{\langle \beta_n \rangle}$



To see the relationship between the $N_{n,i}$ for different n , consider first the relationship between the $n = 2$ and $n = 3$ cases. First observe that $N_{0,2} \subseteq N_{0,3}$ where, concordantly $E_{2,0} = \mathbb{Q}(\zeta_2) = (\mathbb{Q}(\zeta_2, w_2))^{N_{2,0}} \subseteq (\mathbb{Q}(\zeta_3, w_3))^{N_{3,0}} = \mathbb{Q}(\zeta_3) = E_{3,0}$. For the other $N_{2,i}$ and $N_{3,j}$ we have the following.



We have that $Gal(\mathbb{Q}(\zeta_3, w_3)/\mathbb{Q}(\zeta_1)) = \langle \sigma_3, \beta_3 \rangle$ where $\sigma_3(w_3) = \zeta_3 w_3$ of course, and β_3 generates the Sylow p -subgroup of $Gal(\mathbb{Q}(\zeta_3, w_3)/\mathbb{Q}(w_3))$, which, by natural irrationality, is isomorphic to the Sylow p -subgroup of $Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q})$, namely $Gal(\mathbb{Q}(\zeta_3)/\mathbb{Q}(\zeta_1))$. As such $\beta_3(\zeta_3) = \zeta_3^{\pi^{(p-1)}}$ where π is the primitive root mod p , which we observed earlier is the same for all higher powers of p . And since $w_3^p = w_2$ and $\zeta_3^p = \zeta_2$ then $Gal(\mathbb{Q}(\zeta_2, w_2)/\mathbb{Q}(\zeta_1))$ equals $\langle \sigma_2, \beta_2 \rangle$ where $\sigma_3^p = \sigma_2$. Indeed, $\sigma_3(w_2) = \sigma_3((w_3)^p) = (\zeta_3 w_3)^p = \zeta_2 w_2 = \sigma_2(w_2)$ and similarly $\beta_3(\zeta_2) = \beta_3((\zeta_3)^p) = \zeta_3^{p\pi^{(p-1)}} = \zeta_2^{\pi^{(p-1)}} = \beta_2(\zeta_2)$, that is the action of σ_3 restricts to σ_2 and β_3 to β_2 . As such, for $E_{3,j}$ and $E_{2,i}$ given above, $E_{2,i} \subseteq E_{3,j}$ only when $i = j$. Moreover, we have a natural surjection $N_{3,i} \rightarrow N_{2,i}$ given by $\sigma_3^i \beta_3^p \mapsto \sigma_2^i \beta_2$. In general therefore, by viewing

$Gal(\mathbb{Q}(\zeta_{n-1}, w_{n-1})/\mathbb{Q}(\zeta_1)) \subseteq Gal(\zeta_n, w_n)/\mathbb{Q}(\zeta_1))$ we have the following

Proposition 5.1: *For $Gal(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_1)) = \langle \sigma_n, \beta_n \rangle$ then for $i \in \{0, \dots, p-1\}$ there is containment $E_{n-1,i} \subseteq E_{n,i}$ where $E_{n,i}$ is the fixed field of $N_{n,i}$. Moreover $\{N_{n,i}, \nu_{n,n-1}\}$ (for $n \geq 3$) forms an inverse system where for $i = 0$ $\nu_{n,n-1}(\sigma_n) = \sigma_{n-1}$, and for $i \in U_p$ that $\nu_{n,n-1}(\sigma_n^i \beta_n^{p^{n-2}}) = \sigma_{n-1}^i \beta_{n-1}^{p^{n-3}}$.*

Also, one can observe that $\langle \beta_n \rangle$ normalizes each $N_{n,i}$ so that $N_{n,i}$ is a normal complement to $\langle \beta_n \rangle$ in $Gal(\mathbb{Q}(\zeta_n, w_n)/\mathbb{Q}(\zeta_1))$. Also, since each $N_{n,i}$ is Abelian (and therefore its own opposite) then $\mathbb{Q}(w_n)/\mathbb{Q}(\zeta_1)$ is Hopf-Galois with respect to the action of $H_{n,i} = (E_{n,i}[N_{n,i}])^{\langle \beta_n \rangle}$ where each is a $E_{n,i}$ -form of the group ring $\mathbb{Q}(\zeta_1)[N_{n,i}]$. If we define $\overline{\Delta}_n = \langle \beta_n \rangle$ then we may form the inverse limit $\overline{\Delta}_\infty$ of the system $\{\overline{\Delta}_n, \phi_{n,n-1}\}$ in the same fashion as we used to define Δ_∞ . Similarly, we may define $N_{\infty,i} = \varprojlim N_{n,i}$ and $E_{\infty,i} = \varinjlim E_{n,i}$, and $H_{\infty,i} = \varprojlim H_{n,i}$. In a manner identical to that developed earlier, we have therefore that $\mathbb{Q}(w_\infty, \zeta_1)/\mathbb{Q}(\zeta_1)$ is a Hopf-Galois extension with respect to the action of $H_{\infty,i}$, where $H_{\infty,i} \cong (E_{\infty,i}[N_{\infty,i}])^{\overline{\Delta}_\infty}$ and $E_{\infty,i} \otimes H_{\infty,i} \cong E_{\infty,i}[N_{\infty,i}]$. This shows that the non-uniqueness of the Hopf-Galois structures which may act on a given extension holds for infinite extensions such as these.

References

- [1] D. L. Armacost and W.L. Armacost. On p-thetic groups. *Pacific Journal of Mathematics*, 41(2):295–301, 1972.
- [2] S. Caenepeel. *Brauer Groups, Hopf Algebras and Galois Theory*. K-Monogr. Math. Kluwer Academic, 1998.
- [3] S.U. Chase and M. Sweedler. *Hopf Algebras and Galois Theory*. Number 97 in Lecture Notes in Mathematics. Springer Verlag, Berlin, 1969.
- [4] L. Fuchs. *Abelian Groups*. Springer Monographs in Mathematics. Springer, 2015.
- [5] C. Greither and B. Pareigis. Hopf galois theory for separable field extensions. *J. Algebra*, 106:239–258, 1987.

- [6] R. Hagenmüller and B. Pareigis. Hopf algebra forms of the multiplicative group and other groups. *Manuscripta Math.*, 55:121–136, 1986.
- [7] T. Kohl. *Classification of Abelian Hopf Algebra Forms Acting on Radical Extensions*. PhD thesis, 1996.
- [8] T. Kohl. Classification of the hopf galois structures on prime power radical extensions. *J. Algebra*, 207:525–546, 1998.
- [9] B. Pareigis. *Descent Theory Applied to Galois Theory, technical report*. Univ. of California, San Diego, 1986.
- [10] C. Webb. Tensor and direct products. *Pacific Journal of Mathematics*, 49:579–594, 1973.